

CLAIMS

We claim:

1. A method of using a computational effort invested in a proof of work (POW), comprising: distributing a task among a plurality of entities; receiving a POW relating to said task from one of said plurality of entities; and using said POW to accomplish said task.
2. The method of claim 1 further comprising using said POW to accomplish a security goal.
3. The method of claim 1 wherein distributing said task among a plurality of entities includes partitioning said task into a plurality of sub-tasks and distributing each one of said plurality of sub-tasks to a respective one of said plurality of entities.
4. The method of claim 1 wherein said security goal involves restricting resource access by said one of said plurality of entities.
5. A method of using a computational effort invested in a proof of work (POW), comprising: partitioning a minting operation into a plurality of sub-tasks; distributing one of said plurality of sub-tasks to one of a plurality of entities; receiving a POW from said one of said plurality of entities; and using said POW to accomplish said minting operation.
6. The method of claim 5 further comprising using said POW to accomplish a security goal.
7. The method of claim 5 wherein said minting operation includes identifying valid solutions that hash to a predetermined image and wherein said POW represents a valid solution.

8. The method of claim 6 wherein said predetermined image comprises a range of images.
9. The method of claim 8 wherein all images within said range of images have a predetermined number of least significant bits in common.
10. The method of claim 5 wherein each of said sub-tasks comprises searching a different solution search space for valid solutions.
11. The method of claim 6 wherein said security goal involves restricting resource access.
12. The method of claim 7 further comprising verifying said valid solution by determining whether said valid solution represented by said POW hashes to said predetermined image.
13. A method of using a computational effort invested in a proof of work (POW) comprising: distributing a minting operation among a plurality of entities in a manner that maintains privacy in said minting operation; receiving a POW from said one of said plurality of entities relating to said minting operation; and using said POW to accomplish said minting operation.
14. The method of claim 13 further comprising using said POW to accomplish a security goal.
15. The method of claim 13 wherein said minting operation comprises using a hash function to identify a predetermined number of valid solutions that hash to a target value and wherein said POW represents a valid solution.

16. The method of claim 15 wherein said predetermined number of valid solutions comprise a coin.

17. The method of claim 15 wherein said predetermined number of valid solutions hash to a portion of said target value.

18. The method of claim 13 wherein said distributing includes instructing each of said plurality of entities to search within a different search space for valid solutions.

19. The method of claim 15 wherein said privacy is maintained in said minting operation by keying said hash function with a secret value.

20. The method of claim 19 wherein said secret value includes a portion specific to a coin.

21. The method of claim 20 wherein said secret value includes a portion specific to a period of said coin's validity.

22. The method of claim 19 wherein said hash is of a concatenation of a solution and a value generated using said secret value.

23. The method of claim 13 further comprising verifying said POW.